GÖTEBORGS UNIVERSITET

Användandet av icke-sanktionerade molnapplikationer inom svenska organisationer

The use of non-sanctioned cloud applications within Swedish corporations

Micael Samuelsson

Mastersuppsats i informatik

Rapport nr. 2014:088
ISSN: 1651-4769

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2014

Sammanfattning

Molnapplikationer som DropBox har under de senaste åren blivit allt mer populära och erbjuder anställda möjligheten att kunna kommunicera och dela filer mellan varandra. För att få en förståelse för hur icke-sanktionerade molnapplikationer används påbörjades en undersökning för att identifiera risker och möjligheter för svenska organisationer.

Denna uppsats genomfördes med en kvalitativ ansats och inleddes med en litteraturstudie som följdes av nio stycken intervjuer med personer som har erfarenhet av IT-infrastruktur och Cloud Computing. Resultatet indikerade att IT är intressant för organisationer där man önskar ha en bättre kontroll över kostnader och resurser samt kunna förändra vid behov. Om organisationer inte implementerar en policy för hur icke-sanktionerade molnapplikationer ska hanteras kan anställda välja att skapa sina egna regler och att man därför tappar kontrollen över data.

Genom att analysera och se över sina nuvarande behov kan organisationer behålla kontrollen över data, samtidigt som man undviker att det blir dyrare och kan minska kostnader samt skala sina resurser beroende på behov.

Exempelvis kan framtida forskning vara att man undersöker hur användningsscenariot ser ut på arbetsplatsen kontra hemma och vad det är för typ av resurser som behövs inom organisationen.

Nyckelord: BYOD, BYOA, Cloud Computing, Outsourcing, molnet.

Göteborgs Universitet
Institutionen för tillämpad Informationsteknologi
Göteborg, Sverige, Maj 2014

Abstract

Cloud Applications such as DropBox has in recent years become increasingly popular and offer employees to communicate and share files between each other. To get an understanding of how nonsanctioned cloud applications used initiated a study to identify risks and opportunities for Swedish organizations.

This essay was carried out with a qualitative approach, which began with a literature study followed by nine interviews with people who have experience in IT infrastructure and Cloud Computing. The result indicated that cloud computing is interesting for organizations in which they wish to have a better control of costs and resources, and be able to change if necessary. Furthermore, the results pointed to if you do not wish to risk organizations that employees choose to create their own rules and therefore lose control of the data .

By organizations analyze and review their current needs, they can maintain control over the data, while avoiding the costs and can reduce costs and scale their resources depending on the needs.

For example, future research is to investigate how usage scenario looks at work versus at home and what type of resources needed in the organization.

Keywords: BYOD, BYOA, Cloud Computing, Outsourcing, Cloud-applications

Förord

Jag vill börja med att tacka min handledare Dick Stenmark som har uppmuntrat, motiverat och guidat mig. Utan mina respondenters tid och deltagande hade det varit svårt att genomföra denna uppsats. Därför vill jag rikta ett stort tack för att de har delat med sig av deras tid och kunskap.

Göteborg, 2014-05-25

Micael Samuelsson

Innehållsförteckning

Introduktion till användandet av icke-sanktionerade molnapplikationer

Bakgrund

De flesta organisationer använder system, applikationer och programvaror av olika slag. Det arbete som har utförts av anställda inom organisationer har gett upphov till vad det är som behöver lagras. Detta har traditionellt sett lösts av organisationer med att köpa in hårdvara och programvaror till de anställda, där datorhallar hanterade fil- och applikationsservrarna. Vilka system eller applikationer som anställda hade tillgång till beslutades av organisationen eftersom de betalade för datorer och licenser.

Inom 1990-talet uppstod outsourcing, vilket innebar att organisationer kunde lägga ut ansvaret för hanteringen av data, till exempel det som tidigare hanterades i datorhallar till andra organisationer (Marions och Briscoe, 2009). Detta kan ske på grund av att man vill minska sina kostnader eller få tillgång till ny teknologi med stordrift. Tanken bakom detta var att andra kunde hantera data under tiden som man fokuserade på sin kärnverksamhet.

Detta ledde senare till att företag insåg att man med molntjänster kunde köpa programvaror som en tjänst och att det inte behövdes några licenser eller servrar att installera programvaran på. Företagen bestämde vilka anställda som fick tillgång till sina applikationer och system (Rittinghouse och Ransome, 2010). Detta hanterades i molnet och det som behövdes beställdes av organisationer. Detta ledde till att mobilitet blev allt mer populärart och laptops kompletterades med handdatorer som till exempel Compaq Ipaq.

Molnteknologier utgör ett alternativ för utbyggnad av IT-resurser eftersom resurserna levereras över nätet och är åtkomliga för användarna via olika typer av klienter. Molnet fokuserar på att få ut effektiviteten för användaren med resurser och flexibilitet. De är inte delade mellan användare utan fördelas också vid behov. En europeisk server kan fördela resurser till en amerikansk server vid behov under dagtid i Amerika (Rittinghouse och Ransome 2010). Vidare är molnet är mer etablerat och användas i smartphones, surfplattor och laptops. Inte bara Apple, Google och Microsoft erbjuder tjänster utan det finns även andra leverantörer som erbjuder tjänster till exempel Amazon.

Vilket möjliggjorde fenomen som Bring Your Own Device (BYOD), där anställda tillåts att ta med tablets, smartphones eller laptops till jobbet och användas (Weiss, 2007). Dropbox och andra molntjänster används för samarbete mellan anställda för att de ses om smidiga och produktivitetshöjande. (Chaudhry, 2012))

Alla är inte lika entusiastiska över den tekniska utvecklingen. Anställda kan inte ha kontroll över de säkerhetsaspekter som berörs av Bring Your Own Device (BYOD) eller användandet av molntjänster och applikationer. Därför är det viktigt ur ett management perspektiv för ett företag att bestämma om support skall ges på applikationer eller tjänster som man själva inte levererar.

Vidare har inte organisationer insyn i hur data hanteras när den läggs upp i molnet, därför går det inte att veta vilken server eller var den sparas. Ledningen som tidigare har haft ansvaret för denna typ av frågor har fått se situationen förändras när andra tillhandahåller tjänster som man själv tidigare har ansvarat för. Vad tycker de om denna utveckling? Vilka risker har de identifierat och vad kan de göra åt dem? Vad har de upptäckt för möjligheter och hur kan de säkerställa att detta utvecklas?

Syfte med studien

Syftet med denna uppsats är att undersöka hur IT-ansvarige inom svenska organisationer ser på användandet av icke-sanktionerade molntjänster. Detta ska genomföras med intervjuer om organisationers syn på icke-sanktionerade molnapplikationer och tjänster och en genomgång av molnteknologier.

Denna studie ämnar här besvara följande frågeställning:

> Hur ser organisationer på användandet av icke-sanktionerade tredjeparts molntjänster?

Teoretiskt ramverk

IT Management

Informationsteknik management (IT-management) är den process där resurser som är knutna till informationsteknik hanteras efter organisationens prioriteringar och behov (Magoulas och Pessi, 1998). Detta inkluderar materiella resurser som nätverksprodukter, datorer och människor, samt immateriella resurser som programvara och data. Det centrala målet för IT-förvaltningen är att skapa värde genom användning av tekniken och långsiktigt utveckla IS/IT (Henderson och Venkatramn, 1991). Detta innebär att man skall arbeta för att förbättra skyddet på produkter, tjänster och kundrelationer (Buchta och Eul, 2010) För att uppnå detta måste affärsstrategier och teknik anpassas (Magoulas och Pessi, 1998).

Organisationer kan mäta, kontrollera och hantera IT-infrastruktur för att kunna leverera kvalitativa, kostnadseffektiva tjänster för att möta både kortsiktiga och långsiktiga behov som finns för applikationer och tjänster (Orand, 2011).

Under 1960 förutsåg organisationer att ett system skulle täcka alla behov. Ansvar för IT-funktioner hamnade lokalt, samtidigt som den centrala ledningen hade mindre ansvar, ledde till ett större behov av att fokusera på kärnverksamheten och att outsourca det som inte sågs som en del av ens kärnverksamhet (Magnusson, 2010).

Outsourcing

Outsourcing, kan beskrivas som att en annan verksamhet tar över en del av verksamheten och driver det åt en (Wendell och Klepper, 1998). Grover, et al (1994) menar att IT Outsourcing handlar om användandet av externa tjänsteleverantörer för att kunna leverera process, applikationer- och infrastrukturslösningar till företag.

Outsourcing kan ske på grund av att kostnader behöver minskas och att leverantören tillhandahåller bättre effektivitet, resurser och tillgång till nyare teknologi (Amiti, M och Jin-Wei S, 2004). Tidigare har det varit svårare att leverera tjänster externt på grund av begränsad bandbredd, när detta förändrades kunde tjänster med mer bandbredd till exempel Cloud Computing levereras externt (Rittinghouse och Ransome, 2010).

Cloud Computing

Traditionellt sett har organisationer köpt in programvaror som licenser, vilka har hanterats och underhållits av lokal IT (Armbrust et al, 2010). Den organisation som väljer att frångå licenser och istället köpa in det som en tjänst upprättar ett avtal med leverantören om vilkoren (Rittinghouse och Ransome, 2010). Beroende på vilken typ av avtal det är som man upprättar, kan delar eller hela verksamheten använda sig av molnet.

Molnet är något som kontinuerligt utvecklas och därför kan definitionen av molnet skilja sig åt. Några menar att molnet handlar om en skalbar tjänst där den drivs av virtualiserade servrar och blir tillgänglig för sina användare vid behov (Rittinghouse och Ransome, 2010, Vaquero et al 2009). För organisationer ger denna bättre skalbarhet och användning av resurserna, vilket ger billigare resurser. Rittinghouse och Ransome (2010) menar att detta gör att molnet bättre klarar av att tillhandahålla effektiva resurser för användare oberoende av tid. Exempelvis klarar molnet av att ett datorcentrum går ner eftersom ett annat har backup (Rittinghouse och Ransome, 2010).

IASA (2009) menar att Cloud Computing karakteriseras av enorma resurser och används vid behov av kunder, där det levereras externt. Även om definitionerna av molnet varierar bland användare och organisationer är många överens om att det handlar om skalbarhet och bättre användning av existerande resurser. Rittinghouse och Ransome (2010) menar att molnet är gammalt men att det börjar bli allt populärare eftersom användare får tillgång till mer bandbredd. Applikationer tillhandahålls vid behov för användare, där betalning sker efter hur mycket tjänsten används eller vilka resurser som organisationer behöver

Software as a service (SaaS)

Software as a service ses som ”on-demand software”, där applikationer tillhandahålls vid behov. Detta som en del av ”Cloud Computing” där även andra tjänster som Infrastructure as a Service (IaaS) och Platform as a Service (PaaS) ingår.

SaaS används efter ”pay-per-use”, där betalning sker efter hur mycket tjänsten används. Applikationerna kan kommas åt via en tunn klient eller webbläsare. Exempel på denna typ av applikationer som används vid dessa scenarios är Office, Management, CAD, virtualisering och ERP programvaror. Enligt Rosen et al (2008) finns det två olika sätt som organisationer kan välja att betala för sitt användande: Hur mycket man använder sig av systemet eller per användare. Det finns även möjlighet för organisationer att förändra sina behov

Risker och Cloud Computing

Enligt Thomson (2012) har allt fler enheter till exempel smartphones, laptops och tablets åtkomst till känsliga data, vilket ökar risken för organisationer eftersom man inte vet vad det är för typ av icke-sanktionerade applikationer eller tjänster som är installerade.

Wright et al (2012) och Semer (2013) menar att organisationer kan motverka risker genom att dela upp anställdas enheter i två delar. En del som innehåller företagshemligheter och den andra innehåller privatinformation, till exempel applikationer. Wright et al (2011) menar att risken ökar eftersom organisationer inte har möjlighet att kontrollera vad det är för typ av icke-sanktionerade applikationer eller tjänster som är installerade på anställdas personliga enheter.

Chaudhry (2012) och Hudson (2012) menar att anställda tar med sig molnapplikationer som exempelvis DropBox, Google Drive eller OneDrive till arbetsplatsen när de tar med personliga enheter. Enligt Chaudhry (2012) har företag inte kontroll över deras data när anställda använder sig av exempelvis DropBox eller andra icke-sanktionerade tjänster på personliga enheter eftersom de inte vet hur hanteringen sker. Om det är så att organisationer har implementerat Mobile Device Management policy för hur applikationer skall hanteras menar Wright et al (2011) och Chaudhry (2012) att risker kan motverkas. En MDM metod är en "best practice metod" där organisationer kan reglera säkerheten för anställdas privata- och företagsenheter.

MDM funktionalitet omfattar vanligtvis over-the-air distribution av program, data och inställningar för alla typer av enheter. Detta gäller såväl företagsägda och personalägda (BYOD) enheter i hela företaget eller mobila enheter som ägs av konsumenterna. Problemet för organisationer vid sådana tillfällen är att avgöra vad det är som är fel? Genom att implementera en MDM policy menar Rose (2013) att organisationer förhindra vilken typ av icke sanktionerad enhet eller applikation som får åtkomst till organisationens data.

Chaudhry (2012) menar organisationer som inte anpassar sig till Bring Your Own Device och att anställda väljer att ta med sig personliga enheter råkar ut för större risker eftersom de kan välja att skapa egna regler för användande av personliga enheter och hur data skall hanteras med icke-sanktionerade applikationer.

Bring Your Own Device (BYOD)

BYOD eller Bring Your Own Device handlar om hur anställda kan ta med sina egna enheter (till exempel telefoner, tablets eller laptops) till arbetsplatsen och använda dem till känslig information och applikationer på arbetsplatsen (Kestle R och Self R, 2013). Fördelen för organisationer är att kostnader för abonnemang och hårdvara fördelas till de anställda (PC Magazine, 2012). Nackdelen är att det skapar en större börda på organisationen eftersom det är svårare att säkra och supportera hårdvara och tjänster som man inte äger (Lohrmann, 2013).

BYOD tillåter användare att använda sig av icke sanktionerade programvaror eller tjänster på sina privata datorer eller telefoner (Barkhus L, 2005). Denna effekt är mer känd som Bring Your Own Software eller Bring Your Own Application (Computer Sweden, 2013). Fördelen med detta är att organisationer kan få ett större engagemang och produktivitet från sina anställda när de får ta med sig egna laptops, smartphones eller tablets. Nackdelen är att säkerheten blir mer problematisk, exempelvis kan inte data säkras på samma sätt om den lagras externt jämfört om man hade sparat det på interna lagringsplatser.

Med Bring Your Own Application ökar behovet på organisationers interna service för att supportera icke-standardiserade enheter eller applikationer. Om en anställd får sin enhet stulen finns det möjlighet att rensa den externt, men det finns ingen sådan lösning för att rensa molnet om andra skulle få åtkomst. För att hantera icke-sanktionerade applikationer kan organisationer introducera policys som gäller för att deras personliga enheter ska få tillgång till det interna nätverket (CIO, 2013).

Enligt en studie utförd av McAfee (2013), väljer över 80 procent av anställda sina egna software-as-a-service (SaaS) lösningar. Anställda väljer att använda sig av icke-sanktionerade molnapplikationer av tre anledningar:

- De föredrar applikationer som de själva har valt framför sådant som är officiellt sanktionerat
- Dessa programvaror eller tjänster hjälper bättre till i arbetet
- Med molnteknologi och möjligheten att komma åt sina applikationer från olika webbläsare är det enkelt för anställda att själva välja sina egna applikationer.

Till exempel kan detta handla om att anställda väljer att använda sig av DropBox, OneDrive, iCloud eller Google Drive för att föra filer mellan sin arbetsdator och hemdator. Detta ökar komplexiteten för IT-avdelningar eftersom man inte har kontroll över hur informationen hanteras (Lunde och Mattson, 2012). Vilket inte är enbart

negativt utan låter organisationer upptäcka nya applikationer som kan förbättra produktiviteten (CIO, 2013).

Företag behöver utarbeta en policy för hur de skall hantera situationen när anställda använder sig av andra program eller tjänster än de som officiellt stöds eftersom data kan replikeras och att det saknas möjlighet att vet hur det hanteras när till exempel Dropbox, iCloud eller OneDrive används (Chaudry, 2012). En organisation kan sätta upp Mobile Device Managent (MDM) strategi för att hantera säkerhet och behålla kontroll över data när icke-sanktionerad applikationer används. Semer (2013) menar att denna typ av policy gör att organisationer bibehåller kontroll över data samtidigt som den anställde får ha sin egna personliga enhet.

Organisationer som inte skapar denna typ av policy för sin organisation tar större risker eftersom anställda kan välja att skapa egna regler för hur data skall hanteras (Chaudry, 2012). Denna policy skall inkludera rekommendationer från IT, ekonomi och HR. Dock behöver organisationer vara medvetna om implementation av en policy är både tids- och ekonomiskt krävande (Thomson, 2013). Risken är att om denna typ av policy saknas, kan anställda lämna organisationen med känslig data på sina personliga enheter. Därför är det viktigt att chefer och andra avdelningar inom organisationen är överens gällande regler och policys innan man tillåter användandet av personliga enheter inom organisationen (Zielinski, 2012).

Metod

En studies forskningsmetod handlar om insamling och analys av data. Vilken typ av undersökningsmetodik som används baseras på studiens problemområde och frågeställning. Syftet är att ta en bit av ett större fall och låta det beskriva verkligheten. Detta kan komma från ett mindre förlopp som beskriver verkligheten, till exempel hur ett beslut tas inom en organisation (Patel och Davidson, 2003). Enkäter, intervjuer eller observationer kan användas för att samla in data för studier (Bryman, 2013).

När en studie utförs finns det två olika sätt att arbeta, *induktivt* eller *deduktivt*. En deduktiv studie innebär att det utförs en studie där resultatet baseras på befintliga kunskaper och teorier. Om det utförs en induktiv studie är den inte baserad på några tidigare kunskaper, där resultatet ska ge ny teori (Bryman, 2008).

Denna studie har genomförts med ett *deduktivt* förhållningssätt, där den litterära studien och empiriska insamlingen har skett efter en iterativ process. Jacobsen (2007) menar att ett deduktivt förhållningssätt påverkas av den existerande kunskapen som forskaren har. Detta kan vara att studiens öppenhet minskas och att frågornas utformning påverkas av forskarens tidigare kunskap.

Initialt genomfördes det en förstudie med en av mina respondenter där det ställdes öppna frågor. Denna del var tänkt att utföras *induktivt*, men eftersom jag har använt mig av molnapplikationer både privat och i arbetet kunde det inte utföras.

Det empiriska materialet för denna studie har samlats in genom nio intervjuer med IT-strateger och IT-arkitekter, baserade inom större svenska företag. Respondenternas olika roller och tidigare erfarenheter bidrar till denna uppsats tillförlitlighet eftersom de har insyn i hur organisationens nuvarande och kommande IT-satsningar ser ut.

Praktiskt tillvägagångssätt

I början läste jag in mig på problemområdet för att kunna studera molnteknologier, där även andra begrepp som Bring Your Own Device (BYOD), Bring Your Own App (BYOA), Bring Your Own Service (BYOS) och Cloud Computing studerats.

Denna förstudie genomfördes med hjälp av Google Scholar, Göteborgs Universitetsbiblioteksdatabaser med fokus på databasen Inspec. Utöver detta har sökmotorer som Bing och Google använts för att samla in information som inte har täckts av de vetenskapliga databaserna. Nyckelfraser som ”skiften i molnet”, ”molnets utveckling”, ”BYOD historia” "Bring Your Own Device” och engelska motsvarigheter har använts.

Detta utfördes med ett deduktivt angreppssätt, där existerande teorier och forskningsmetoder används för att stärka studien och kunna upptäcka likheter och skillnader. Därefter utformades den empiriska studien med hjälp av kunskaperna från förstudien.

Intervjufrågor

Frågorna i denna studie har fastställts och diskuterats med min handledare. Innan intervjuerna utfördes blev mina respondenter informerade om vilka frågor som skulle ställas för att de skulle kunna förbereda sig.

De frågor som ställdes under intervjuerna utformades för att täcka olika aspekter av synen på användandet av icke-sanktionerande tredjeparts molnapplikationer av IT-ansvarige.

Genomförande av intervjuer

För denna uppsats intervjuade jag nio olika personer som har olika IT-roller inom svenska organisationer. De respondenter som arbetade i Göteborg intervjuades på sin arbetsplats och med deras tillåtelse spelades de in.

Om mina respondenter inte har varit baserade i Göteborg har en tid överenskommits för en intervju över Skype alternativt telefon och med respondenternas tillåtelse har intervjuerna spelats in för att kunna analyseras i efterhand. Var och en av intervjuerna tog mellan 30 – 60 minuter och delades upp i fyra olika avsnitt.

Intervjuerna var semistrukturerade för att frågorna skulle kunna skifta plats vid behov. Detta kan ses som nödvändigt för att man inte alltid kan mötas på samma grunder och att det därför kan skapa bättre kommunikation (Patel och Davidson, 2003)

Respondenterna kommer att nämnas som ”Respondent A” eller ”Respondent B” efter intervjuordning.

Personer med insyn och erfarenhet av IT-infrastruktur och Cloud Computing har intervjuats för att kunna besvara uppsatsens forskningsfråga.

Respondenter och bakgrundsinformation

För att studiens syfte och forskningsfråga skall kunna besvaras behövdes personer med insikt i hur organisationer ser på användandet och hanterandet av icke sanktionerade moln-applikationer. Detta urval består av personer som jobbar med IS- och – IT relaterade frågor på svenska organisationer.

Denna förstudie syftade till att ge insikt om hur det kommande arbetet skulle baseras, hur IT-ansvarige inom svenska organisationer ser på användandet av icke-sanktionerade molnapplikationer och en grund för kommande tankar och idéer under arbetets utförande.

På grund av en personlig relation och tidigare erfarenhet av Cloud Computing och IT-infrastruktur valdes Respondent A ut för den initiala förstudien. Efter den initiala förstudien med Respondent A valdes respondenterna ut *ändamålsorienterat* efter sin tidigare erfarenhet och kunskap om IT-infrastruktur, molnapplikationer och Cloud Computing (Jacobsen, 2002).

Respondent A
Respondent A arbetar som *enterprise architect* med frågor gällande IT-infrastruktur på ett större svenskt företag inom mjukvarubranschen. Han har som uppgift att koordinera och sätta upp IT-infrastrukturen för att se till så att allt fungerar och sköts enligt planerna. Organisationen har som mål att konsolidera IT-användningen och sänka sina kostnader. Han har tidigare erfarenhet av att jobba med infrastrukturfrågor inom Sverige och internationellt.

Respondent B
Respondenten arbetar för närvarande som *CTO* för ett större företag inom hårdvaru- och mjukvarubranschen. Målet för deras organisation är att få de olika avdelningarna att arbeta bättre ihop och minska de gemensamma kostnaderna för deras organisation. Han är även aktiv inom organisationer som Svenska IT-Arkitekter Sverige (IASA-Sverige).

Respondent C
Respondenten arbetar för närvarande på IT-avdelningen som *System Analyst* för ett större svenskt företag som har verksamhet Hon har tidigare erfarenhet av att jobba inom Service Desk och 2: nd line utveckling för interna och externa projekt inom företaget.

Respondent D
Respondenten jobbar för närvarande som *Team Leader (TL)* för en extern Service Desk, där han ansvarar för den dagliga verksamheten och att SLA uppnås enligt satt avtal med deras externa kund. I detta avtal behöver han ha se till att den dagliga verksamheten fungerar på Service Desk löser ärenden samt att andra avdelningar följer SLA.

Respondent E
Respondenten arbetar som *CIO* på ett större svenskt företag inom IT-branschen. Målet för deras organisation är att attrahera nya kunder inom olika branscher för att växa företaget.

Respondent G
Respondenten arbetar för närvarande som *Teknisk Evangelist* inom ett större företag i hårdvaru- och mjukvarubranschen. För närvarande arbetar respondenten som *strategisk rådgivare och utvecklare* åt organisationer för att de skall använda sig av deras system för den dagliga verksamheten.

Respondent H
Respondenten arbetar för närvarande med IT-baserade frågor, där målet är att supportavdelningen skall outsourcas och att organisationen skall fokusera på kärnverksamheten. Han är även utnämnd till Most Valuable Professional av Microsoft för sitt arbete med Microsoft Azure.

Respondent I
Respondenten arbetar efter för närvarande med ett eget konsultföretag där han arbetar med molnteknologier, utveckling och IT-infrastruktur. Han är även utnämnd till Most Valuable Professional av Microsoft. Han har tidigare erfarenhet av att jobba med IT relaterade frågor både inom och utanför Sverige.

Analys
Det empiriska resultatet har strukturerats efter de tre områden som min forskningsfråga belyser: 1) IT Management, 2) Outsourcing och 3) Bring Your Own Device (BYOD). För att kunna skapa en bättre överblick över hur IT ansvarige ser på användandet av icke sanktionerade molnapplikationer har resultatet delats in i underkategorier som har identifierats efter analys av det empiriska resultatet. Resultatet av den empiriska studien har tematiserats i citatform och text för att kunna återskapa hur respondenterna agerade och uttryckte sig under intervjuerna.

Resultat

Outsourcing

Resultat av intervjuerna med mina respondenter visar att det inte finns en tydlig bild av Outsourcing och Cloud Computing. Fyra av mina respondenter anser att Cloud Computing och Outsourcing är samma typ av tjänst. Respondent H säger följande *" Molnet är en vidareutveckling av Outsourcing. Med hjälp av molnet kan vi få minskade kostnader eftersom organisationen inte behöver ha sina egen infrastruktur utan vi kan jobba överallt och prestera bättre. Risken är att vi fortfarande inte vet allt om det och att det kontinuerligt utvecklas. Detta är farligt för organisationer eftersom det är bra för dem idag behöver det inte betyda att det är bra för de om några månader eller år.*".

Fem av mina respondenter anser att det är två skilda tjänster eftersom Outsourcing handlar om företag och utveckling, där Cloud Computing handlar om möjligheten att jobba överallt på samma villkor. Respondent G berättade under intervjun *" Molnet är en ny typ av tjänst som kontinuerligt utvecklas, [OS] handlar mer om företag och hur delar av deras verksamhet drivs av andra. Det är inte så att vi skall låta andra ta över delar av vår verksamhet utan det handlar mer om att vi behöver kunna jobba överallt och då är molnapplikationer ett bättre val för oss istället för [OS]*".

Molntjänster

Nästan alla av mina respondenter var överens om att Cloud Computing handlar om hur individer eller organisationer använder sig av konsument- eller företagsapplikationer till exempel DropBox eller SkyDrive för att hantera data på sin privata- eller arbetsdator. Respondent I berättade *att "Cloud Computing är en tjänst vilket tillåter organisationer eller personer att arbeta mot en plattform eller applikation till exempel DropBox eller OneDrive. Skalbarhet gör att vi kan anpassa det efter organisationens behov, till exempel minskar antalet anställda behöver vi inte ha lika mycket resurser. "*.

Två av mina respondenter menade att Cloud Computing är ett nätverk av tjänster där man med hjälp av avtal kan konfigurera det för att fungera med olika typer av organisationer. Respondent B berättade under intervjun *" Cloud Computing innebär förändringar för organisationer, det introducerar nya sätt att arbeta för anställda. Organisationer behöver bara knyta ihop vilka tjänster som ska användas och vilka resurser som skall finnas tillgängliga för anställda om de behöver hjälp eller guidning. Den stora utmaningen för organisationer är att anställda att läsa igenom*

avtalen som följer med vid personliga- och företagsapplikationer. Det gäller att varje person och organisation läser igenom för att man skall förstå vilka risker och möjligheter som finns i att använda till exempel DropBox, SkyDrive eller annat. ".

Användandet av molnapplikationer

Resultatet visar att det finns en fragmenterad syn på användandet av icke-sanktionerade molnapplikationer inom svenska organisationer. Fem av mina respondenter menade att de använder sig av olika typer av molnapplikationer för kommunicera med användare externt och inom organisationen. Detta är något som uppmuntras av ledningen eftersom det är viktigt att varje individ känner till hur applikationerna fungerar och att de har möjligheten att jobba överallt med både företagets- och personliga enheter. Respondent B berättade följande om hur det fungerar *"Ledningens uppmuntran att lära oss ny teknologi och applikationer har gjort att vi har möjligheten att prestera och må bättre. Sen har allt det andra med säkerhet och utveckling följt med på köpet eftersom vi har möjlighet att använda oss av de enheter som anställda känner för. Om vi inte hade tillåtit molnapplikationer inom vår organisation hade anställda förmodligen försökt att hitta vägar runt och förmodligen lyckats".*

Fyra av mina respondenter berättar att de för närvarande använder sig av molntjänster genom Office 365 som är kopplat till OneDrive Pro. Detta lämpar sig bra för deras organisationer eftersom det inte finns något behov av en existerande infrastruktur utan anställda kan jobba överallt. Respondent C berättade följande *"Med hjälp av integration av Office 365, Windows 8 och OneDrive Pro tillåter vi anställda att jobba överallt och vi vet att det är säkert. Windows 8, Windows Phone 8 och OneDrive Pro är de enda kraven vi har om anställda vill arbeta med personliga enheter istället för de vi tillhandahåller. Detta har hittills varit ett framgångsrikt koncept eftersom vi har anammat BYOD istället för att säga nej. Hade vi sagt nej hade anställda istället skapat sina egna regler, vilket hade förändrat situationen eftersom vi hade tappat kontrollen över data".*

Förmodligen kan säkerheten vara lika bra i molnet enligt Respondent A men innan de har fastställt det är det inte tillåtet att använda sig av molnapplikationer. Dock påpekade han att de arbetar med detta successivt eftersom det är viktigt att besluten blir rätt när det kommer till säkerhet och integration. Respondent I berättade följande *"Om en anställd skulle använda sig av en icke-tillåten applikation utan att vi vet om riskerna skulle anställningen avslutas omedelbart. Det är endast ok att använda en applikation som DropBox eller OneDrive när den är godkänd av ledningen efter att vi har gått igenom hur den påverkar vår organisation. Förmodligen använder sig våra anställda av olika applikationer som DropBox redan nu men det är inget som vi kan*

påverka, det enda vi kan göra är att visa vilka applikationer som vi anser är ok att användas inom organisationen".

Fördelar med användande av molntjänster

Fem av mina respondenter berättade att de använder konsumentapplikationer som DropBox, Google Drive eller OneDrive för att kommunicera med externa kunder om filerna ses som icke-känsliga. De är medvetna om att applikationerna kan vara icke tillåtna inom andra organisationer, men användandet av molntjänster som DropBox eller OneDrive är något som uppmuntras av ledningen för att anställda skall veta hur IT-infrastruktur och Cloud Computing fungerar. Respondent B menade att det handlar om lärande efter användande, om anställda inte använder sig av molnapplikationer som DropBox eller OneDrive har de inte möjlighet att lära sig funktionaliteten.

Respondent H berättade följande "*Fördelen för organisationer som tillåter användandet av molntjänster är att man inte behöver utbilda anställda en gång till, de vet redan hur man skall använda sig av molnapplikationer. Hade vi behövt utbilda anställda inom organisationen hade situationen sett annorlunda ut, till exempel hade man inte kunnat räkna med lika stora kostnadsfördelar.* "

Om filerna bedöms som känsliga använder de sig av OneDrive Pro eftersom Microsoft erbjuder organisationer information om hur deras data hanteras. Respondent B sa under intervjun: "Det *finns inga risker, bara möjligheter med [C C]. Allt handlar om hur organisationer tillåter anställda att använda sig av applikationer för att jobba. Bedöms filerna som känsliga använder vi oss av OneDrive Pro annars kan man använda sig av [DB] eller [OD] för filer som ses som allmänna. Bedöms filerna kunna hittas via Google eller Bing är det helt okej att använda sig av DropBox eller OneDrive ".*

Tre av mina respondenter berättade att de använder sig av konsumentapplikationer som DropBox eller OneDrive för att dela filer med sina kunder. Om filerna innehåller företagshemligheter använder de sig av andra metoder till exempel OneDrive Pro eller mail för att dela filer mellan användare inom och utanför organisationen. Respondent H berättade följande " *Organisationer har bara möjligheter, det finns inga nackdelar med molnet. Det gäller bara att vet hur man skall använda det. Jag har gått in i andra organisationer och förkastat deras tankar om molnet och visat dem hur man skall använda sig av molnapplikationer. Detta har förändrat deras tankesätt om hur man skall arbeta och interagera*".

Respondent B berättade: *”Detta kanske inte ses som tillåtet av andra men det beror på vad det är för typ av filer som man delar externt med andra. Det jag gjorde var att fundera ut vad jag ville dela, hur jag ville dela och vad innebar det för risker. Visst tog detta lång tid men det gjorde att jag hade en plan, vilket godkändes av ansvariga inom min organisation eftersom både de och jag visste vad det var för risker som jag utsatte mig för. Hade jag inte varit öppen med mina planer hade andra saker kunnat hända under mitt arbete”:*

Nackdelar med molntjänster

Nästan alla av mina respondenter berättade att den stora svagheten med Cloud Computing är hur filer hanteras när konsumentapplikationer som OneDrive eller Dropbox används inom deras organisation. Detta är något som mina respondenter var överens om måste ordnas innan de kan tillåta användandet. Respondent B berättade följande: "*Den stora svagheten med molnapplikationer till exempel DropBox eller OneDrive är att det inte finns möjlighet att veta hur data hanteras. Detta är vad som organisationer är för när det kommer till molnapplikationer, det saknas möjlighet att kontrollera vad anställda gör när de använder sig av applikationen. Just detta gör att organisationer bli osäkra och inte vet hur de skall hantera att molnapplikationer används. Flertalet anställda använder sig säkert idag icke-sanktionerade molnapplikationer men det är inget vi kan kontrollera. Därför gäller det att hitta ett sätt som är sanktionerat*.".

Tre av mina respondenter menade att det behöver slutas ett avtal med leverantören innan de kan tillåta användandet av molnapplikationer inom sina organisationer. Respondent J berättade: *”Möjligheten att veta hur organisationens data hanteras har gjort att vi har slutit avtal med Microsoft gällande OneDrive Pro. Innan vi tog detta beslutet utvärderade vi andra alternativ men fann att de andra alternativen som DropBox, OneDrive eller Google Drive inte gav oss möjligheten att vet hur data hanteras när de används”.*

Respondent G berättade under min intervju om användandet av icke tillåtna konsumentapplikationer: "*Skulle jag se att en av mina anställda använder sig av icke tillåtna konsumentapplikationer till exempel [DB] eller [OD] skulle jag ta de i örat och varnas. Är det ett upprepat beteende att en icke auktoriserad konsumentapplikation används kan anställningen avslutas omedelbart och personen är inte välkommen att återkomma. Detta är inte något som har hänt ännu i vår organisation, men jag tror att det kommer hända någon gång och då gäller det att veta hur en sådan situation ska hanteras*".

Respondent H menade att det inte finns några risker när en organisation tillåter användandet av icke sanktionerade molnapplikationer utan det handlar om vilka typer av filer som man laddar upp. För organisationer är det viktigt att Personuppgiftslagen (PUL) och svenska lagar följs enligt Respondent H eftersom det ger ett skydd kring hur data hanteras och vad organisationer kan förvänta sig när de tillåter konsumentapplikationer inom sina organisationer.

Bring Your Own Device (BYOD)

Alla av mina respondenter var överens om att Bring Your Own Device handlar om att organisationer kan ta med sig en personlig enhet, till exempel telefon eller laptop för att använda på arbetsplatsen. Respondent C berättade följande om användandet av Bring Your Own Device *”Policys kan skilja sig åt beroende på vilken organisation det handlar om men rent generellt sett handlar detta om att man kan ta med sig personliga enheter till exempel smartphones eller tablets till sin arbetsplats och använda de precis som man sitter hemma utan restriktioner”.*

Respondent H berättade ”*Bring Your Own Device är ett intressant koncept eftersom anställda kan ta med sig egna smartphones och använda på arbetsplatsen. Fördelen är att organisationer inte behöver stå för kostnaderna på abonnemanget eller hårdvaran. Nackdelen är att organisationer tappar kontrollen över data, vilket gör att man inte vet men som har tillgång till den eller hur den hanteras”.*

Användande av Bring Your Own Device inom svenska organisationer

Tre av mina respondenter berättar att Bring Your Own Device är något som används inom deras organisation och uppmuntras av ledningen eftersom de har möjlighet att skifta sina egna kostnader från hårdvara och abonnemang till att stödja den anställde med finansiella medel förutsatt att enheten uppfyller de krav som ställs från organisationen. Respondent C berättar följande "*Anställda inom organisationen kan köpa laptops från till exempel Asus eller Lenovo om de känner för det, enda kravet är att de måste installera en image på datorn som följer de krav som organisationen ställer på anställdas datorer. Jag köpte själv en dator från Lenovo, som följer mina och organisationens krav på datorer*".

Två av mina anställda menade att de använder sig av smartphones och laptops som deras organisationer tillhandahåller. Enheterna är konfigurerade så att varje anställd inte kan installera egna program utan behöver beställa programvaror via ett internt beställningssystem. Respondent A berättade följande "*Nackdelen med detta system som min organisation tillhandahåller är att jag tar med mina egna tablets och smartphones. De som vi tillhandahålls har jag ingen möjlighet att göra något annat än*

arbete, vilket gör att jag försöker hitta vägar runt systemet. Till exempel har jag konfigurerat min företags epost på min iPhone för att jag inte ska behöva bära med min företagstelefon på fritiden om jag vill arbeta".

Fördelar med Bring Your Own Device

Respondent H berättade att deras organisation har frihet under eget ansvar, där anställda tillåts att installera egna molnapplikationer efter en obligatorisk utbildning. Drär han berättade följande om hur det fungerar: *"Anställda måste utbildas i risker och möjligheter med icke tillåtna konsumentapplikationer, när de har genomgått utbildningen tillåts de att använda DropBox eller OneDrive. Om det inte har genomgått denna utbildning är det förbjudet att använda sig av molnapplikationer eftersom anställda inte vet om risker och fördelar".*

Respondent A menade att *"Bring Your Own Device är ett suveränt koncept eftersom jag har möjlighet att ha ny teknologi tillsammans den senaste säkerheten inom organisationen. Andra länder har anammat detta mer inom sina organisationer, vad säger att vi inte kan ha det här i Sverige? Detta är nya tider och det blir svårare för organisationer som inte försöker hänga med. Säger en organisation nej till Bring Your Own finns det en risk av att anställda skapar sitt egna program och då tappar man kontrollen över både regler och data".*

Respondent C menade att organisationer som tillåter användandet av icke-sanktionerade molnapplikationer inte behöver utbilda sina anställda i funktionalitet eftersom anställda har erfarenhet från att använda applikationer som DropBox eller OneDrive hemma. Respondent H berättade följande: *"Jag tror det bara kommer bli större, andra länder har det i större kapacitet vad säger att vi inte kan ha det här i Sverige? Säkerhet och utveckling går hand i hand. Hade vi valt att säga nej till detta hade anställda inom organisationen valt att skapa sina egna regler och då hade vi tappat kontrollen över datan. Till exempel tillhandahåller vi en lista på vårt intranät där vi beskriver vilka applikationer som får och inte får användas. Givetvis kan de använda de icke-sanktionerade ändå, men detta är till för att guida anställda ett steg i rätt riktning.".*

Risker med Bring Your Own Device

Alla mina respondenter var överens om att tillåta Bring Your Own Device (BYD) och egna applikationer innebär utmaningar när det kommer till kompabilitet, support, administration och licenser. Respondent C berättade *"Organisationer kan behöva hjälpa till med support av de tjänster eller enheter som de själva inte tillhandahåller*

eftersom de har tillåtit BYOD förväntar sig anställda att de kan komma för att få support när applikationer inte fungerar så som det är tänkt".

Tre av mina respondenter menade att organisationer som tillåter användandet av konsumentapplikationer inte släpper på sina existerade säkerhetskontroller utan att man bryter mot dem eftersom man saknar insyn i hur applikationer som DropBox eller OneDrive är uppbyggda. Respondent G berättade följande *"Organisationer som tillåter Bring Your Own Device får det tufft eftersom ansvariga saknar möjligheten att kontrollera vad det är som finns installerat på anställdas enheter. Om en organisation implementerar en MDM strategi kan man få bättre översyn över anställdas enheter. Alternativt kan man upprätta ett avtal inom sin organisation, där man beskriver vad som får och inte får göras när anställda väljer att ta med sig egna enheter till arbetsplatsen".* Respondent C berättade *"Organisationer som tillåter BYOD måste vara förberedda på att anställda upplever att de får andra regler än de som är ansvariga. Ansvariga tillhandahålls de enheter som anställda oftast vill ha".*

Respondent J berättade *"Organisationer måste förändra sina säkerhetspolicys att inkludera personliga enheter, där lösenordet skall bytas på personliga enheter och de som organisationen tillhandahåller var 30:e dag. Implementeras inte denna typ av policys riskerar organisationerna att anställda väljer att skapa sina egna regler för hur data skall hanteras".*

Respondent A menade att organisationer behöver bli mer restriktiva när det kommer till användandet av icke tillåtna konsumentapplikationer eftersom man inte vet vad det är för typ av data som varje anställd laddar upp. *"Är man inte insatt i hur molnapplikationer fungerar vet man inte om man laddar upp sina senaste semesterbilder eller arbetsdokument. På grund av detta är det viktigt att anställda får utbildning även om det inte är organisationens tjänster eftersom anställda behöver tydliga direktiv hur de ska hantera risker och användande".*

Respondent J berättade *"Vi kan inte säga nej till att låta anställda ta med sig egna laptops, smartphones eller tablets eftersom detta är något som skulle hända oavsett hur mycket vi säger nej. Därför ser vi till att ha uppdaterade säkerhetspolicys och utbildningar för anställda inom vår organisation. Detta uppskattas av våra anställda eftersom dem vet att de kan ha enheter som de själva har valt och vi vet samtidigt att vårt data är säkrad. ".*

Analys och diskussion

Syftet med min uppsats var att undersöka hur IT-ansvarige inom svenska organisationer ser på användandet av icke-sanktionerade molnapplikationer. Med hjälp av teorier inom Cloud Computing och det empiriska resultatet har jag skapat en grund inför analys och diskussion. Jag kommer i analys och diskussion att diskutera och gå igenom tidigare teori och empiri.

Outsourcing

Resultatet av denna uppsats visar att bilden av Cloud Computing och Outsourcing skiljer sig åt mellan svenska organisationer. Respondent G berättade att molnet är en vidareutveckling av Outsourcing. Outsourcing handlar om att organisationer låter andra organisationer ta över delar av verksamheten och molnet handlar om att varje organisation inte behöver ha en existerande infrastruktur utan kan jobba på olika platser. Detta stämmer överens med Wendell och Klepper (1998) och Grover et al (1994) som menar att Outsourcing handlar om användandet av externa tjänsteleverantörer för att kunna leverera process, applikationer- och infrastrukturlösningar för företag.

Respondent I lyfter fram att molnet och outsourcing är två separata tjänster. Respondent G lyfter fram att molnet är under kontinuerlig utveckling, Outsourcing handlar om att företag tar över delar av verksamheten och driver det åt en. Vidare lyfte Respondent I fram att molnapplikationer är ett bättre val istället för Outsourcing eftersom anställda behöver kunna jobba överallt. Detta stämmer överens med Rittinghouse och Ransome (2010) och Vaquero et al (2009) om att Cloud Computing är under kontinuerlig utveckling och att definitionen kan skilja sig åt bland användare.

Cloud Computing

Resultatet visar att det finns en gemensam förståelse att molnet handlar om att företag eller individer använder sig av molnapplikationer till exempel DropBox, Google Driver eller OneDrive för att komma åt specifika tjänster. Detta belyses även av IASA (2009) vilka menar att molnet karakteriseras av enorma resurser och görs tillgängliga för användarna externt vid behov. Andra som Vaquero et al (2009) och Rittinghouse och Ransome (2010) menar att Cloud Computing handlar om en skalbar tjänst, där den drivs av virtualiserade servrar och görs tillgängliga för användarna vid behov.

Respondent I lyfter fram att Cloud Computing låter användare att med hjälp av applikationer komma åt specifika tjänster, till exempel DropBox eller OneDrive på sin privata- eller arbetsdator. Detta stämmer överens med Armbrust et al (2010) att

organisationer kan välja att köpa in applikationer som tjänster istället för att köpa in som programvaror som licens.

Intervjuerna med mina respondenter visar att det finns en skillnad i hur molnapplikationer tillåts att användas inom svenska organisationer. Organisationer kan uppmuntra sina anställda att använda sig av molnapplikationer som DropBox, Google Drive eller OneDrive för kommunicera med kunder. Där andra säger att de inte tillåts att använda icke-sanktionerade applikationer inom organisationen, men de använder icke-sanktionerade applikationer ändå för arbete.

Fördelar med Cloud Computing

Tidigare nämndes att användare eller organisationer kan använda sig av molnapplikationer för att komma åt specifika tjänster till exempel DropBox eller OneDrive. En viktig aspekt för att skifta till molnapplikationer är att det finns möjligheter för organisationer att spara pengar eftersom de inte behöver ha en egen infrastruktur. Detta belyses även av Gorssman och Helpman (2002) som menar att molnet bygger på en virtualiserad miljö, där leverantörens kunder delar på den existerande infrastrukturen och betalar efter vad det är som används (Rosenet al, 2008).

Magoulas och Pessi (1998) lyfter fram att organisationer kan prioritera resurser efter behov. Detta stämmer överens med resultatet från min empiriska studie som visar att organisationer kan välja att tillåta icke-sanktionerade molnapplikationer när de vet hur det fungerar med existerande infrastruktur.

Tidigare nämnda skalbarheten utgör enligt mina respondenter ett incitament för organisationer att skifta till molntjänster och applikationer eftersom varje organisation kan anpassa sina resurser efter deras behov. Detta innebär att organisationer kan skala sina resurser upp eller ner beroende på vilket typ det är som man har inom organisationen. Detta stämmer överens med Rosen et al (2008) som menar att organisationer kan betala för sitt behov efter antal användare eller hur mycket varje organisation använder sig av systemet.

Nackdelar med Cloud Computing

Resultatet pekar på att organisationer inte har möjlighet att kontrollera hur data hanteras när användandet inte tillåts inom organisationen. Detta stämmer överens med Chuadry (2012), Ross (2013) och Hudson (2012) som menar att risken ökar när anställda har med sig personliga enheter till exempel smartphones eller tablets eftersom organisationen inte tillåter att de tar med sig personliga enheter, vilket gör att

de tappar kontrollen över data. Respondent G berättade att om han skulle se en av sina anställda använda sig av en icke sanktionerade molnapplikation skulle de först varnas, är det upprepat beteende menade han att personens anställning inom organisationen kan avslutas omedelbart.

Risken med att inte låta anställda installera egna applikationer är att de skapar sina egna regler för hur de ska användas inom och utanför tjänsten. Respondent J berättade att de inte kan säga nej till att anställda tar med sig egna applikationer eller enheter utan det gäller att ha utbildningar och uppdaterade säkerhetspolicys för organisatioens anställda för att motverka risker. Exempelvis menar Chuadry (2012) att risker ökar för organisationer eftersom det inte finns möjlighet att kontrollera vad det är för icke-sanktionerade applikationer som anställda har installerat på sina enheter.

Ett sätt att komma runt problematiken med att organisationer inte vet hur data hanteras är att sluta ett avtal med en leverantör som Respondent J gjorde med Microsoft och OneDrive Pro. Detta avtal gjorde att deras organisation standardiserade hur molnapplikationer skulle hanteras av anställda och man visste hur data hanterades inom och utanför organisationen. Detta för med sig en annan problematik eftersom anställda kan välja att använda sig av andra icke-sanktionerade molnapplikationer innan ett avtal har slutits.

Bring Your Own Device (BYOD)

Bring Your Own Device handlar om att anställda kan ta med sig en personlig enhet exempelvis smartphone, dator eller tablet till arbetsplatsen och använda den.Detta stämma överens med Kestle och Self (2013) som menar att anställda får tillgång till känslig information när de tar med sig en personlig enhet till arbetsplatsen. Respondent C menade att Bring Your Own Device kan skilja åt beroende på organisationer eftersom till exempel ledningen inom organisationer inte har samma regler som anställda eftersom då är mer benägna att ha med sig en egen iPhone eller iPad till arbetsplatsen.

Oberoende om organisationen tillhandahåller enheter för sina anställda eller att anställda väljer att med sig personliga enheter, kommer de att användas utanför organisationen. I likhet med teorin Lunde och Mattson (2012) och Thomson (2013) visar resultatet att implementationen av en Bring Your Own Device policy inom svenska organisationer innebär utmaningar. Som McAfee (2013), Barkhus (2005) och Lohrmann (2013) antyder är risken med BYOD att anställda installerar icke sanktionerade molnapplikationer till exempel DropBox, Google Drive eller OneDrive på sina personliga enheter.

Enligt intervjuerna med mina respondenter är detta en risk eftersom organisationer behöver förändra sina existerande policys inom organisationen för att fungera ihop med Bring Your Own Device eftersom man annars bryter mot dem. Respondent H menade att om anställda inte är insatta i hur molnapplikationer fungerar föreligger det en risk då man inte vet om man laddar upp semesterbilder eller arbetsdokument.

Fördelar med Bring Your Own Device

En fördel med att tillåta Bring Your Own Device inom organisationer är att anställda tar över kostnaden för abonnemang och hårdvara. Nackdelen för organisationer är att man inte har möjlighet att tillhandahålla support för alla programvaror som organisationens anställda använder sig av. Detta stämmer överens med Barkhus (2005) som menar att anställda kan installera programvaror som inte tillåts av organisation. Denna effekt är mer känd som Bring Yur Own Application eller BYOA.

Ett sätt att tillåta och överbrygga problematiken med molntjänster är enligt Respondent H att utbilda anställda i risker och fördelar med molnapplikationer i ”frihet under eget ansvar”. Om anställda inte har genomgått denna utbildning menade Respondent H att anställda inte får använda sig av molnapplikationer som DropBox eller OneDrive. Detta stämmer överens med Chaudry (2012) och Thomson (2013) att företag behöver utarbeta en policy för hur användandet av molnapplikationer skall hantera. Denna typ av policy låter företag bibehålla kontrollen över data samtidigt som den anställda får ha med sig sin personliga enhet (Semer, 2013).

En annan intressant aspekt är när Respondent C tar upp att organisationer inte behöver utbilda sina anställda i hur applikationer som DropBox eller OneDrive fungerar eftersom anställda har erfarenhet av att använda denna typ av applikationer hemma. Detta ökar komplexiteten för organisationer eftersom man kan tvingas supportera applikationer som inte tillhandahålls av organisationen för att kunna kontrollera hur data hanteras av externa leverantörer. Detta stämmer överens med Barkhus (2005) som menar att Bring Your Own Device låter användare att installera programvaror inte tillhandahålls av organisationen.

Nackdelar med Bring Your Own Device

Resultatet visar att Bring Your Own Device eller BYOD innebär utmaningar när det kommer till support, kompabilitet, administration och licenser för organisationer. Respondent C lyfter fram att organisationer kan behöva hjälpa anställda med support och administration för att veta hur data hanteras eftersom när anställda tar med egna enheter tar de ofta med egna applikationer. Detta stämmer överens med Lunde och

Mattson (2012) som menar att komplexiteten för organisationer ökar eftersom man saknar kontroll över hur data hanteras.

Resultatet visar en intressant aspekt nämligen att organisationer som tillåter Bring Your Own Device inom sina organisationer bryter inte mot sina existerande säkerhetspolicys utan släpper på dem eftersom man inte vet hur data hanteras. Ett sådant scenario kan en organisation motverkas genom att implementera en Mobile Device Managmenet strategi, ofta sett som en ”Best Practice” metod. I denna strategi ska organisationer sätta upp hur icke-sanktionerade applikationer skall hanteras för att säkerhet och kontroll skall kunna bibehållas (Semer, 2013 och Chaudry, 2012).

En annan aspekt är att organisationer som väljer att säga nej till att låta användare ta med sig egna enheter får ökade risker eftersom anställda kan välja att skapa egna regler för hur data skall hanteras. Detta stämmer överens med vad Semer (2013) säger om att organisationer som inte implementerar en policy kring BYOD löper större risker eftersom anställda skapar sina egna regler istället.

Förslag på fortsatt forskning

För att visa ytterligare en dimension i hur molnapplikationer används inom svenska organisationer hade det varit intressant att ta fram ett ramverk eller en modell för hur icke-sanktionerande molnapplikationer ska användas. Detta kan exempelvis inkludera säkerställandet av att molnapplikationer ska följa de regler som finns inom organisationen för att anställda ska kunna använda molnapplikationer.

Vidare kan det vara av intresse att undersöka skillnaderna i hur molnapplikationer som DropBox eller OneDrive används av anställda och ansvariga inom svenska organisationer, genom att studera skillnaden i hur molnapplikationer används på arbetsplatsen och hemma.

Slutsats

Syftet med denna uppsats är att belysa hur IT-ansvarige inom svenska organisationer använder sig av icke-sanktionerade molntjänster, samt vilka möjlighet och risker som icke-sanktionerade molnapplikationer utgör. Frågeställningen löd:

- Hur ser organisationer på användandet av icke-sanktionerade tredjeparts molntjänster?

Från uppsatsens teoretiska ramverk och analys och diskussion har slutsatser dragits. Nedan följer detta fördelat på fördelar och risker med icke-sanktionerade molnapplikationer inom svenska organisationer.

Fördelar med icke-sanktionerade molntjänster

Molnapplikationer har med sin modell potentialen att erbjuda bättre kontroll av resurser och kostnader, förutsatt att varje organisation har bestämt sig för att tillåta användandet av molnapplikationer som DropBox, OneDrive eller Google Drive. Fördelen med detta är för organisationer att man kan skifta kostnader för hårdvara och abonnemang till anställda. Detta gör att organisationer kan prioritera sina resurser efter behov. Detta kan leda till att verksamheten passar bättre ihop med IT.

Organisationer som tillåter användandet av molnapplikationer som DropBox, Google Drive, iCloud eller OneDrive kan minska sitt fokus på de delar som inte ses som kärnverksamhet, till exempel kan det vara möjligheten att jobba överallt på personliga enheter och de som tillhandahålls av organisationen.

När användaren tar med sig personliga enheter tar de ofta med sig egna applikationer exempelvis DropBox eller OneDrive. För att organisationen ska behålla kontrollen över data på användarens personliga enheter kan de implementera en Mobile Device Management policy för att kontrollera säkerhet och vad det är för applikationer som anställda har installerat.

Om filerna bedöms som publika och inte innehåller företagshemligheter kan anställda använda sig av exempelvis DropBox, iCloud eller OneDrive för att kommunicera. Bedöms filerna som känsliga får man använda sig av email eller OneDrive Pro eftersom Microsoft ger möjligheten att spåra hur data hanteras. Om en organisation sluter avtal med en extern leverantör gällande molnapplikationer gäller det att man ser över avtalet mellan användare och leverantör för att säkerställa att gällande lagar efterföljs.

Risker med icke-sanktionerade molntjänster

Innan organisationer tillåter användandet av molnapplikationer som tjänster behöver ansvariga se över den nuvarande strukturen och att det inte blir en utmaning för organisationen att applikationerna används. Dock kan det vara så att behoven inom organisationen passar ihop med de utmaningar som uppstår av att man tillåter användandet av molnapplikationer.

Hanterandet av data försvårar för organisationer att tillåta användandet av molnapplikationer som DropBox eller OneDrive. Därför är det viktigt för organisationer att man följer upp vad som händer med data genom att införa en säkerhetspolicy där man informerar om hur molnapplikationer på bästa sätt skall hanteras efter en ”best practice” modell. I denna policy skall det ingå rekommendationer från HR-, IT- och ekonomiavdelningen. Nackdelen med detta är för organisationer att man måste supportera programvaror som man inte tillhandahåller vilket kan innebära ökade risker och att man tappar fokus på andra delar av sin verksamhet.

Om en organisation inte implementerar en säkerhetspolicy riskerar man att anställda skapar egna regler samt att organisationen riskerar att förlora kontrollen av data och inte vet vad det är för typ av data som anställda laddar upp. Exempelvis kan detta vara att anställda väljer att använda sig av applikationer som inte har tillåtits av organisationen.

Organisationer behöver säkerställa att den nuvarande strukturen inte är för komplex och att behoven täcks av att tillåta användandet av icke-sanktionerade molnapplikationer. Annars riskerar man att tillåta system alternativt applikationer som DropBox eller OneDrive, där organisationen inte är förberedd för möjligheter eller risker.

Referenser

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I och Zaharia, M (2010) A View of Cloud Computing. *Communications of the ACM*, 53 (4), pp. 50 -58

Amiti M och Jin-Wei S (2004) Fear of Service Outsourcing: Is it justified? *International Monetary Fund*

Backman J (2008) *Rapporter och Uppsatser*. Studentlitteratur.

Barkhus L (2005) "Bring Your Own Laptop unless You Want to Follow the Lecture" : the Case of Wired Technology in the Classroom. *University of Glasgow*

Bryman A (2008) *Samhällsvetenskapliga metoder*. Liber AB

Buchta D, Eul M och Schulte-Croonenberg (2007) Strategic IT-Management Increase Value, Control Performance, Reduce Costs *Deutsche National Bibliotek*, 2nd edition

Chaudhry, P. (2012) Needed: a corporate mobile device policy, *Financial Executive; Morristown*, 28(5), 69-70

Cio (2013) *Bring Your Own Applications* Tillgängligt på http://www.cio.co.uk/insight/devices/bring-your-own-applications/ Senaste besökt: 2014-04-12

Computer Sweden (2013) *Definitioner* Tillgängligt på: http://cstjanster.idg.se/sprakwebben/ord.asp?ord=bring%20your%20own%20applications senaste besökt 2014-04-10

Davidson, B & Patel , R (2003) *Forskningsmetodikens grunder*. Studentlitteratur

Desisto P R och Pring B (2009) Key Issues for Software as a Service. *Gartner Inc*.

Henderson, J.C. & Venkatramn, N. (1999), Strategic alignment: Leveraging information technology for transforming organizaitons, *IBM systems Journal*, Vol. 36, Nos. 2 & 3

Jacobsen D.I. (2007) *Förståelse, beskrivning och förklaring -- Introduktion till samhällsvetenskaplig metod för hälsovård och socialt arbete*. Studentlitteratur

Jones W.O och Krepper R (1998) Outsourcing information technology, systems and services. *Prentice Hall Inc*.

Kestle R och Self R (2013) *The Role Of IS Assurance & Security Management* University of Derby

Lohrmann D (2013) BYOD *For You: The Guide to Bring Your Own Device to Work* Amazon Digital Services, Inc.

Lunde F och Mattsson G (2012) *Bring Your Own Device - Risker och Möjligheter*. Lunds Universitet

Magoulas, T och Pessi K(1998), *Strategisk IT management*, Vasastadens Bokbinderi AB.

Marinos A och Briscoe G (2009) Community Cloud Computing. *First International Conference, CloudCom* 2009, Beijing, China, December 1-4, 2009. Proceedings

Mcafee (2013) *Bring Your Own Device and mobile Endpoints Are Changing Everything* Tillgängligt på http://www.mcafee.com/uk/resources/solution-briefs/sb-byod-mobile.pdf Senast besök 2014-04-12

Orand B och Villarreal J (2011) *Foundations IT Service Management with ITIL* ITILyaBrady.com; 2 edition

PC Magazine (2013) *BYOD should include BYOS* Tillgänglig på http://www.pcmag.com/article2/0,2817,2418427,00.asp Senast besökt: 2014-04-10

Rittinghouse, J.W. och Ransome, J.F. (2010). *Cloud Computing: Implementation, Management and Security*. Boca Raton, Florida: Taylor and Francis Group, LLC.

Rosen M, Lublinsky Boris, KT och Balcer M J (2008) *Applied SOA: Service-Oriented Architecture and Design Strategies*. Wiley Publishing

Semer, L (2013) Auditing The BYOD Program, *The Internal Auditor*, ISSN 020-5745, 02/2013, 70 (1), 23

Sobragi C.G., Gastaud Macada, A.C. och Oliveira M (2014) Cloud Computing Adoption: A multiple case study. *Revista de Administração e Contabilidade da Unisinos*

Svenska IT-Arkitekter Sverige (IASA) *Sveriges IT arkitekter publicerar definition för Cloud Computing* Tillgänglig på: http://www.iasa.se/?p=267 Senast besökt 2014-04-17

Thomson R.M (2013) Cloud Computing: Constitutional and Statutory Privacy *Protections Congressional Research Service*

Vaquero, L.M., Rodero-Merino, L., Caceres, J. och Lindner, M. (2009) A Break in the Clouds: Towards a Cloud Definition, *ACM SIGCOMM Computer Communication Review*, 39 (1), 50 -55

Weiss A (2007) Computing in the clouds. *Networker*

Zielinski, D. (2012) Bring Your Own Device - More employers are allowing employees to use their own technology in the workplace. *HRMagazine*, ISSN 1047-3149, 02/2012, 57(2), 71.

Bilaga 1 – Begreppslista

Bring Your Own Device (BYOD) - hänvisar till den möjligheten som tillåter anställda att ta personligt ägda mobila enheter (bärbara datorer, tabletter och smarta telefoner) på sin arbetsplats, och att använda dem för att få tillgång till privilegierad företagsinformation och applikationer.

Bring Your Own Service (BYOS) - bygger vidare på Bring Your Own Device (BYOD) och låter anställda att ta med egna applikationer att användas på arbetsplatsen.

DropBox - erbjuder moln lagring, synkronisering fil och klientprogramvara. Dropbox tillåter användare att skapa en särskild mapp på var och en av sina datorer, som Dropbox synkroniserar sedan så att det verkar vara samma mapp (med samma innehåll) oavsett vilken dator används för att visa det. Filer placeras i denna mapp är också tillgänglig via en webbplats och mobiltelefon.

Google Drive - en fil och synkroniseringstjänst som släpptes av Google under 2012, vilket tillåter molnlagring, fildelning och samarbete. Filer som delas allmänt på Google Drive kan hittas via Google.

Molnet (Cloud Computing) – distribuerade resurser över internet vilka man komma åt vid applikationer eller klienter. Kan även beskrivas som att man har tillgång till en gemensam pool av konfigurerbara datorresurser (till exempel nätverk, servrar, lagring, applikationer och tjänster).

Outsourcing – innebär att man låter andra verksamheter ta över och driva en del av sin verksamhet. Detta inkluderar att leverantören kan ta över anställda och tillgångar vid behov om det krävs.

SkyDrive/OneDrive – tjänst som tillåter användare att ladda upp och synkronisera filer till en molnlagring och sedan komma åt dem från en webbläsare eller den lokala enhet. Det är en del av Windows Live utbud av online-tjänster och gör det möjligt för användare att hålla filerna privata, dela dem med kontakter, eller offentliggöra filerna. Offentligt delade filer kräver inte ett Microsoft-konto för tillgång.

Utöver personliga molnlagring, erbjuder Microsoft affärslagring via OneDrive for Business.

Infrastructure as a Service (IaaS) - refereras som en "pay-as-you-go" tjänst där kapaciteten på servern blir tillgänglig för den kund som betalar för det. Denna kapacitet kommer från en datorhall, där leverantören gör den tillgänglig för kunder via internet, klienter eller applikationer.

Platform as a Service (PaaS) – med hjälp av denna modell kan slutanvändare skapa programvaror med hjälp av tjänster från leverantören. Slutanvändaren kontrollerar även utrullning och konfiguration av programvaran.

Service Level Agreement (SLA) – ett avtal som styr servicenivån mellan kund och leverantör. Detta avtal innefattar en lägstanivå av vad kunderna kan förvänta sig av avtalet och vad som händer ifall leverantören inte lyckas nå upp till nödvändig nivå.

Software as a Service (SAAS) - Software as a service refereras som ”on-demand software”, där både programvara och data finns på en server. Detta som en del av ”Cloud Computing” där även andra tjänster som Infrastructure as a Service (IaaS) och Platform as a Service (PaaS) ingår.